DZero VO Services

Parag Mhashilkar,

Tanya Levshina

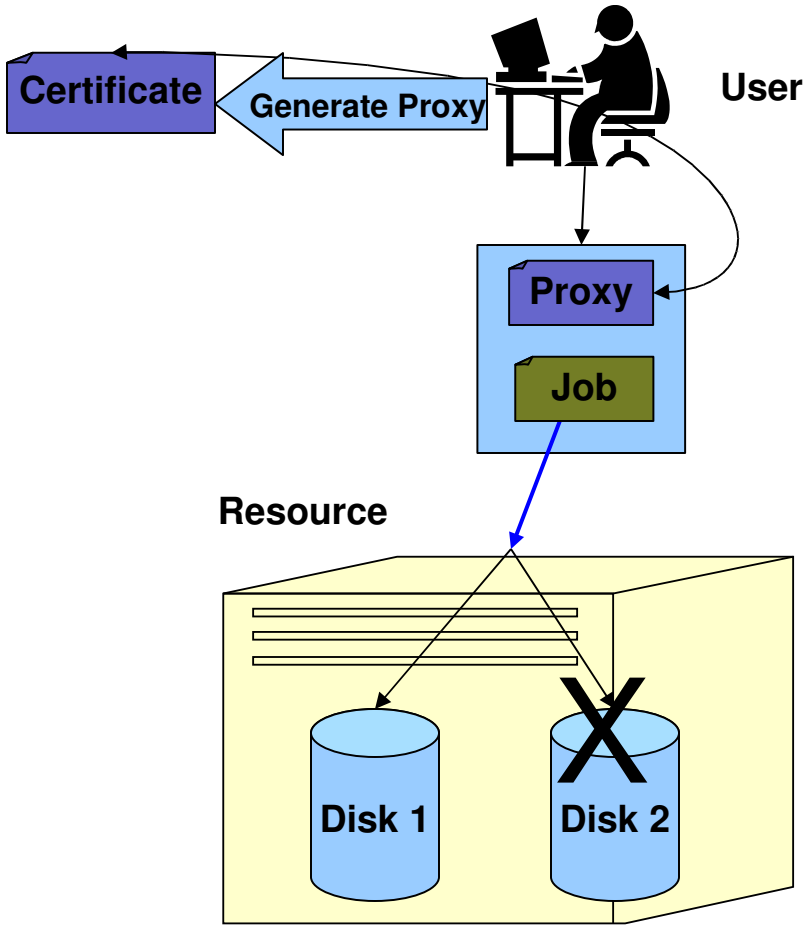
Fermi National Accelerator Laboratory

Overview

- Authentication and Authorization over Grid
- Virtual Organization (VO)
- VO Management Tools
- Motivations for using VOMS/VOMRS
- VO Registration using VOMRS for Dzero
- VO Membership expiration/deletion
- Additional Info

Authentication and Authorization Over Grid

- **Certificate**
  - User credential or identity in digital form. Combination of Public key and Private Key.
- **Certificate Authority (CA)**
  - A Certificate Authority is a trusted third party, which certifies Public Key's to truly belong to their claimed owners.
- **Proxy**
  - Short lived credentials, derived from the certificate.
  - Different types: Full proxy, Delegated proxy, Limited proxy.
- **Authentication**
  - Authentication is any process by which, a system verifies the identity of a user who wishes to access it.
  - In Grids, system can authenticate you if the system supports the CA that issued your certificate.
- **Authorization**
  - Means to control the access level for a system.
  - User may only access some services.

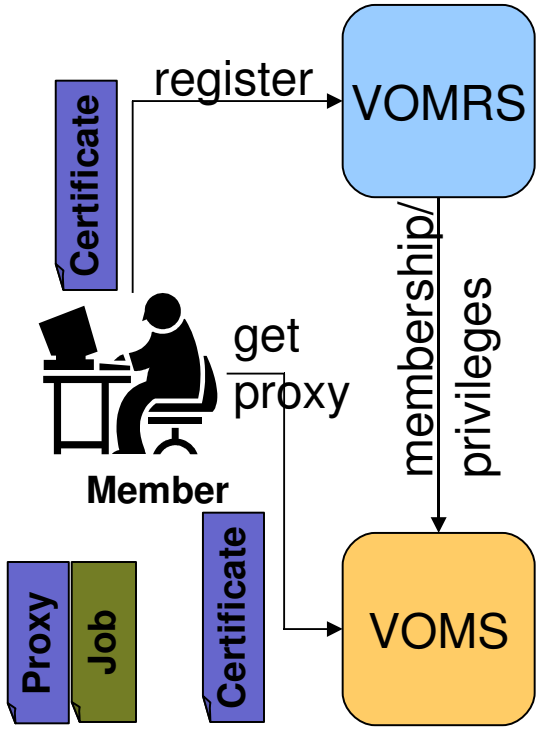


Virtual Organization (VO)

- A Virtual Organization (VO) is a collection of individuals and institutions that agree upon resource sharing on the Grid.
- The VO is responsible for
  - Establishing agreements between the resources providers and the resource users.
  - Maintain the lists of users and services authorized to use the resources of the organization.
- Example:
  - A scientific collaboration, such as the DZero or CDF or MINOS experiment, is generally considered a VO.

VO Management Tools

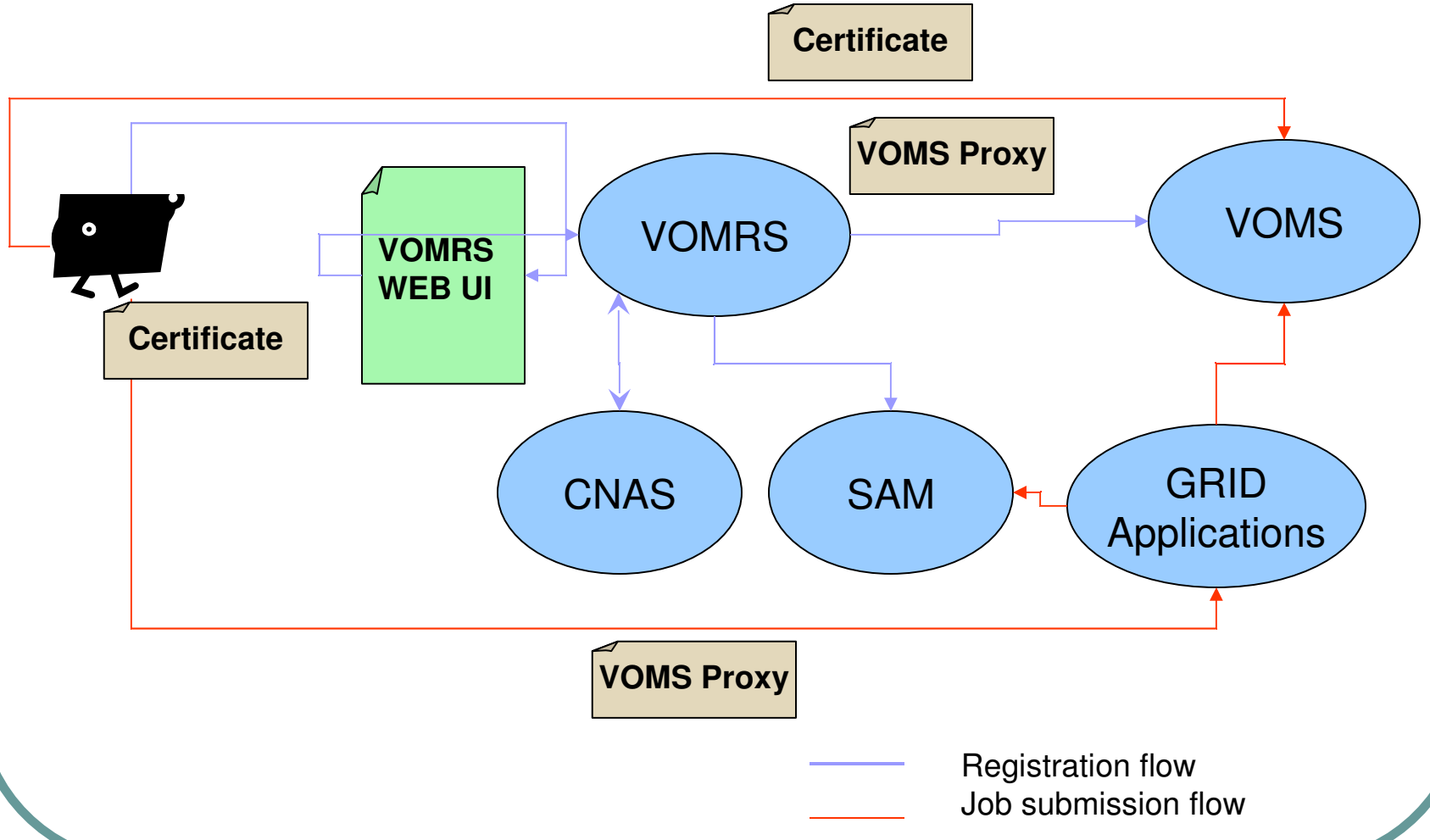
- VOMS
  - VO Management Service for Grid
  - Members with similar properties can be grouped together into same groups and assigned different roles.
  - For DZero we have two sub groups, users and services
  - Users can do 'voms-proxy-init' so that their proxy can be used to represent them as a part of certain sub group or have certain role.
- VOMRS
  - VO Management Registration Service for Grid which interfaces with VOMS.
  - Enhances the registration process.
  - VO's can customize registration process flow and applicant-info collection.



Motivations for using VOMS/VOMRS

- Lack of support for VO specific tools:
  - Site Administrators do not trust the VO customized tools like sam_gsi_config tools to run as root. They prefer to be personally contacted and add new DNs by hand. This is inconvenient and non-scalable. The migration to standard tools will alleviate this problem.
- Combine registration for SAM and Grid Infrastructure into one:
  - Current scheme requires that a user registers twice (sam-user name and DN independently) and that a shifter adds the user's DN to both the SAM database and the sam_gsi_config repository.
- Maintenance
  - All the sam_gsi_config tools are developed in-house by the SAM-Grid team. The focus is on using standard tools.
- Extensibility
  - Standard tools support advance functionalities, such as the extension of user credentials with VO-defined roles. These functionalities are used by authorization services, to provide fine grain authorization to resources. The migration to the standard tools makes it possible for the system to integrate new security services.
- Well Defined Registration Process
  - Applicants can be approved or denied by VO Admin(s) and VO Representatives. This makes it easier to determine the authenticity of the applicant.
  - For DZero: Alan Jonckheere is the VO Admin.

VO Registration process using VOMRS for DZero



User Registration …

- Phase I
  - User provides
    - Basic personal information
    - Email address
    - Fermi Lab Kerberos Principal
    - Selecting SAM groups
    - Verifier's Information
  - VOMRS performs the following actions:
    - Verify the Kerberos principal and assign it to is unique in SAM User Id
    - Register user as a Candidate
- Phase II
  - User confirms email and finishes registration by
    - Selecting VOMS groups
    - Signing usage rule
  - VOMRS performs the following actions:
    - Set user status as Candidate
    - Store Sam groups, VOMS groups, version of signed usage rule

User Registration …

- VO Admin or Representative approves/denies member application
  - If application is approved then
    - If the user exists in SAM and has status active, generate error.
    - If user exists in SAM and has status inactive, register the grid subject and set status active
    - If user does not exist in SAM, add user to SAM.
- Special Case: User does not have Fermilab Kerberos Principal.
  - FNAL security policy requires users of Fermilab resources to have Kerberos Principal. Applicants who do not have Kerberos principal are specially approved by Amber Boehnlein.
    - VOMRS generates SAM User ID for such applicants based on their email address.
- Registering additional certificates
  - Once the VO membership is approved, member can request for registering his/her other certificates through VOMRS.
  - Needs approval from VO admin before the certificates are added to VOMS and SAM.
    - If the user exists, add these certificate subjects to the SAM else generate error.

VO Membership expiration/deletion

- VO Member can no longer a part of VO if -
  - VO admin deletes the user from VOMRS.
  - Membership expires after a certain duration.
    - If user exists in SAM and has status active, then remove the grid subjects from SAMDB and set status inactive

Additional Info

Useful links –

- Design documentation:

http://www-d0.fnal.gov/computing/grid/doc/Samgrid_VO_Proposal.pdf

- DZero VO Registration Page:

https://fermigrid2.fnal.gov:8443/vomrs/vo-dzero/vomrs?

- DZero VO Registration Instructions:

http://www-d0.fnal.gov/VO/DZero_VO_Instructions.html